REMARKS

This response is submitted in response to a Final Office Action mailed January 9, 2008. Claims 1-8 and 10-40 were pending at the time the Office Action was issued. Applicant hereby amends Claims 1, 11, 13-14, 16-18, 22, 28-29, 31-32, 35, and 39. Claims 1-8 and 10-40 remain pending.

I. REJECTIONS UNDER 35 U.S.C. § 102

Claims 1, 8, 10-35, 37, and 39 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. 7,231,516 to Sparrell. Respectfully, Applicant submits that the claims are allowable over Sparrell for at least the reasons explained in detail below.

Claims 1, 8, and 10-16

Claims 8 and 10-16 depend from Claim 1. Claim 1, as amended, recites:

> 1. A method, comprising:
> analyzing a transport stream that includes one or more header portions and one or more corresponding payload portions, each of the header portions includes at least one of a packtetized elementary stream (PES) header and a frame header, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header; and
> preparing the transport stream for a data extraction by encrypting at least some of the payload portions, while leaving the one or more corresponding header portions unencrypted at all times, and generating a multiplex-compliant encryption method packet that at least identifies encrypted portions of the transport stream.

Applicant respectfully traverses this rejection. Specifically, Sparrell does not recite, "generating a *multiplex-compliant encryption method packet* that at least *identifies encrypted portions of the transport stream*," as claimed in Claim 1. (Emphasis added). This claimed element is supported under 35 U.S.C. § 112 by at least Paragraph 27, Lines 6-8, and Paragraph 56, Lines 1-5 of the Specification.

First, while Sparrell discloses multiplexed transport streams, Sparrell does not recite "multiplex-compliant encryption method packets" that identifies encryption portions of a multiplexed transport stream. Specifically, Sparrell discloses that in MPEG-2 multiplexed transport streams, "the stream may be passed through a program identification (PID) filter to select one or more of the component streams." (Column 7, Lines 33-37). However, passing a stream through a PID filter to select one or more component streams is not equivalent to generating a "multiplex-compliant encryption method packet" that is recited in Claim 1.

Second, the "index information" as disclosed by Sparrell also does not recite a "multiplex-compliant encryption method packet" that identifies encryption portions of a multiplexed transport stream. Sparrell discloses an index manager 128 that is "configured to provide index information for the playback of a previously recorded file." (Column 9, Lines 1-3). Specifically, Sparrell further discloses:

> The index manager 128 is responsible for getting the master key from the key manager 130, *decrypting the index file associated with the encrypted data file,* and providing the index and key information to the stream server 134. In the preferred embodiment, the stream server 134 and index manager 128 are processes running on the same CPU and can share this information via shared memory. (Column 9, Lines 3-7). (Emphasis added).

In other words, this portion of Sparrell discloses that the "index information" for the playback of a previously recorded file is stored in an encrypted index file. Further, the index manager 128 is responsible for decrypting the index file to obtain the "index information." However, Sparrell does not recite that that the "index information" is included in a "multiplex compliant encryption method packet," as claimed in Claim 1. Moreover, index information "for the playback of a previously recorded file," is not equivalent to information that "identifies encrypted portions of the transport stream," as claimed in Claim 1.

Third, Sparrell discloses embedding encrypted keys in a media stream. (Column 9, Lines 60-63). Encryption keys are not equivalent to "multiplex-compliant encryption method packets," as claimed in Claim 1. This disclosure of Sparrell also does not recite, "generating a *multiplex-compliant encryption method packet* that at least *identifies encrypted portions of the transport stream*," as claimed in Claim 1. (Emphasis added).

Thus, for at least the above reason, the method recited in Claim 1 is not anticipated by Sparrell. Further, since Claims 8 and 10-16 depend from Claim 1, they are allowable over the cited reference to Sparrell at least due to their dependency, as well as due to additional limitations recited.

Claims 17-21

Claims 18-21 depend from Claim 17. Claim 17, as amended, recites:

> 17. A method, comprising:
> receiving a partially encrypted transport stream that includes one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more encrypted payload portions, wherein each of the

unencrypted header portions enables the processing of the one or more corresponding encrypted payload portions based on at least one of the PES header and the frame header; and

extracting data from the transport stream in a manner that bypasses the one or more encrypted payload portions of the transport stream.

17. A method, comprising:

receiving a partially encrypted transport stream that includes one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more encrypted payload portions, wherein each of the unencrypted header portions enables the processing of the one or more corresponding encrypted payload portions based on at least one of the PES header and the frame header;

generating a multiplex-compliant encryption method packet that corresponds to the transport stream, the multiplex-compliant encryption method packet identifies encrypted portions of the transport stream; and

extracting data from the transport stream in a manner that bypasses the one or more encrypted payload portions of the transport stream.

Applicant respectfully traverses the rejection of Claims 17-21. Specifically, Applicant incorporates the reasoning presented above in response to the rejection of Claim 1 under 35 U.S.C. § 102(e), to the extent that the claims recite the same features, and respectfully submit that Sparrell does not recite "generating a *multiplex-compliant encryption method packet* that corresponds to the transport stream, the multiplex-compliant encryption method packet *identifies encrypted portions of the transport stream*," as claimed in Claim 17. (Emphasis added).

Furthermore, since Claims 18-21 depend from Claim 17, they are at least allowable for the same reasons that make Claim 17 allowable over the cited reference, as well as for additional limitations recited.

Claims 22-30

Claims 23-30 depend from Claim 22. Claim 22, as amended, recites:

> 22. A computer-readable storage medium having one or more instructions that are executable by one or more processors, the one or more instructions causing the one or more processors to:
>
> analyze a transport stream that includes one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more payload portions, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header; and
>
> prepare the transport stream for a data extraction by encrypting at least some of the payload portions while leaving the one or more corresponding header portions unencrypted; and
>
> generate a multiplex-compliant encryption method packet that at least identifies encrypted portions of the transport stream.

Applicant respectfully traverses the rejection of Claims 22-30. Specifically, Applicant incorporates the reasoning presented above in response to the rejection of Claim 1 under 35 U.S.C. § 102(e), to the extent that the claims recite the same features, and respectfully submits that Sparrell does not recite, "generate a *multiplex-compliant encryption method packet* that at least *identifies encrypted portions of the transport stream*," as claimed in Claim 22.

Furthermore, since Claims 23-30 depend from Claim 22, they are at least allowable for the same reasons that make Claim 22 allowable over the cited reference, as well as for additional limitations recited.

Claims 31-34

Claims 32-34 depend from Claim 31. Claim 31, as amended, recites:

> 31. A computer-readable storage medium having one or more instructions that are executable by one or more processors, the one or more instructions causing the one or more processors to:
>
> receive a partially encrypted transport stream that includes one or more unencrypted header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more payload portions, and one or more encrypted payload portions, wherein each of the unencrypted header portions enables the processing of the one or more corresponding encrypted payload portions based on at least one of the PES header and the frame header;
>
> generate a multiplex-compliant encryption method packet that corresponds to the transport stream, the multiplex-compliant encryption method packet identifies encrypted portions of the transport stream; and
>
> extract data from the transport stream based on the one or more unencrypted header portions of the transport stream.

Applicant respectfully traverses the rejection of Claims 31-34. Specifically, Applicant incorporates the reasoning presented above in response to the rejection of Claim 1 under 35 U.S.C. § 102(e), to the extent that the claims recite the same features, and respectfully submit that Sparrell does not recite, "generate *a multiplex-compliant encryption method packet* that corresponds to the transport stream, the multiplex-compliant encryption method packet *identifies encrypted portions of the transport stream*," as claimed in Claim 31. (Emphasis added).

Furthermore, since Claims 32-34 depend from Claim 31, they are at least allowable for the same reasons that make Claim 31 allowable over the cited reference, as well as for additional limitations recited.

Claims 35 and 37

Claim 37 depends from Claim 35. Claim 35, as amended, recites:

> 35. An apparatus, comprising:
> an analyzer to determine which portions of a transport stream are to pass unencrypted, wherein the analyzer identifies one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more payload portions in the transport stream, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header; and
> a scrambler to encrypt at least some of the payload portions while leaving the one or more corresponding header portions unencrypted based on the determination; and
> a generator to generate a multiplex-compliant encryption method packet that identifies encrypted portions of the transport stream.

Applicant respectfully traverses the rejection of Claims 35 and 37. Specifically, Applicant incorporates the reasoning presented above in response to the rejection of Claim 1 under 35 U.S.C. § 102(e), to the extent that the claims recite the same features, and respectfully submits that Sparrell does not recite, "a generator to generate a *multiplex-compliant encryption method packet* that *identifies encrypted portions of the transport stream*," as claimed in Claim 35. (Emphasis added).

Furthermore, since Claim 37 depends from Claim 35, it is at least allowable for the same reasons that make Claim 35 allowable over the cited reference, as well as for additional limitations recited.

Claim 39

Claim 39, as amended, recites:

> 39. An apparatus, comprising:
> means for determining which portions of a transport stream are to pass unencrypted, wherein the analyzer identifies one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more payload portions in the transport stream, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header;
> means for encrypting at least some of the payload portions while leaving the one or more corresponding header portions unencrypted in accordance with the determination; and
> means for generating a multiplex-compliant encryption method packet that identifies encrypted portions of the transport stream.

Applicant respectfully traverses the rejection of Claim 39. Specifically, Applicant incorporates the reasoning presented above in response to the rejection of Claim 1 under 35 U.S.C. § 102(e), and respectfully submits that Sparrell does not recite, "means for generating a *multiplex-compliant encryption method packet* that *identifies encrypted portions of the transport stream*," as claimed in Claim 39. (Emphasis added).

II. REJECTIONS UNDER 35 U.S.C. § 103

Claims 2-7, 36, 38, and 40 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Sparrell in view of U.S. 7,124,303 to Candelore (hereinafter "Candelore").

Claims 2-7

Claims 2-7 depend from Claim 1. Claim 1, as amended, recites:

1. A method, comprising:

analyzing a transport stream that includes one or more header portions and one or more corresponding payload portions, each of the header portions includes at least one of a packtetized elementary stream (PES) header and a frame header, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header; and

preparing the transport stream for a data extraction by encrypting at least some of the payload portions, while leaving the one or more corresponding header portions unencrypted at all times, and generating a multiplex-compliant encryption method packet that at least identifies encrypted portions of the transport stream.

Applicant respectfully traverses the rejection of Claims 2-7. First, Applicant incorporates the reasoning presented above in response to the rejection of Claim 17 under 35 U.S.C. § 102(e), and respectfully submits that Sparrell does not recite, "generating a *multiplex-compliant encryption method packet* that at least *identifies encrypted portions of the transport stream*," as claimed in Claim 1. (Emphasis added).

Second, the deficiencies of Sparrell with respect to this element are not remedied by Candelore. Candelore discloses that audio and/or video packets are encrypted by system A encrypter 218 and system B encrypter 224. (Column 11, Lines 40-44). Candelore further discloses that:

> Once encrypted, these encrypted packets from 218 and 224 are assigned primary or secondary PIDs respectively at 220. System information from 228 and PSI from 229 are multiplexed or combined with the clear packets, the system A encrypted packets and the system B encrypted packets and broadcast over the cable system 32. (Column 11, Lines 43-50).

In other words, while Candelore disclose assignment of packet identifiers (PID) to encrypted packets, Candelore does not disclose that its PIDs are packaged in a

generated "multiplex-compliant encryption method packet." Rather, Candelore discloses that each of the encrypted packets is "tagged" with a PID. (Column 5, Lines 30-35).

Moreover, Candelore further discloses that "system information" is guide data that describes "what programs are available and how to locate the associated channels and components." (Column 3, Lines 12-15). Accordingly, the combination of "system information" and program specific information (PSI) with encrypted packets also does not recite generating a "multiplex-compliant encryption method packet" that "at least *identifies encrypted portions of the transport stream*," as claimed in Claim 1. (Emphasis added).

Thus, the cited references to Sparrell and Candelore, whether individually or in combination, do not teach, disclose, or fairly suggest every aspect of Claim 1. Furthermore, since Claim 2-7 depend from Claim 1, they are at least allowable for the same reasons that make Claim 1 allowable over the cited references, as well as for additional limitations recited.

Claims 36 and 38

Claims 36 and 38 depend from Claim 35. Claim 35, as amended, recites:

> 35. An apparatus, comprising:
> an analyzer to determine which portions of a transport stream are to pass unencrypted, wherein the analyzer identifies one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more payload portions in the transport stream, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header; and

a scrambler to encrypt at least some of the payload portions while leaving the one or more corresponding header portions unencrypted based on the determination; and

a generator to generate a multiplex-compliant encryption method packet that identifies encrypted portions of the transport stream.

Applicant respectfully traverses the rejection of Claims 36 and 38. Specifically, Applicant incorporates the reasoning presented above in response to the rejection of Claim 2-7 under 35 U.S.C. § 103(a). Accordingly, Applicant respectfully submits that the cited references to Sparrell and Candelore, whether individually or in combination, do not teach, disclose, or fairly suggest, "a generator to generate a *multiplex-compliant encryption method packet* that *identifies encrypted portions of the transport stream*," as claimed in Claim 35. (Emphasis added).

Furthermore, since Claims 36 and 38 depend from Claim 35, they are at least allowable for the same reasons that make Claim 35 allowable over the cited references, as well as for additional limitations recited.

Claim 40

Claim 40 depends from Claim 39. Claim 39, as amended, recites:

39. An apparatus, comprising:

means for determining which portions of a transport stream are to pass unencrypted, wherein the analyzer identifies one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more payload portions in the transport stream, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header;

means for encrypting at least some of the payload portions while leaving the one or more corresponding header

portions unencrypted in accordance with the determination; and

means for generating a multiplex-compliant encryption method packet that identifies encrypted portions of the transport stream.

Applicant respectfully traverses the rejection of Claim 39. Specifically, Applicant incorporates the reasoning presented above in response to the rejection of Claim 2-7 under 35 U.S.C. § 103(a). Accordingly, Applicant respectfully submits that the cited references to Sparrell and Candelore, whether individually or in combination, do not teach, disclose, or fairly suggest, "means for generating a *multiplex-compliant encryption method packet* that *identifies encrypted portions of the transport stream*," as claimed in Claim 39. (Emphasis added).

Furthermore, since Claim 40 depends from Claim 39, it is at least allowable for the same reasons that make Claim 39 allowable over the cited references, as well as for additional limitations recited.

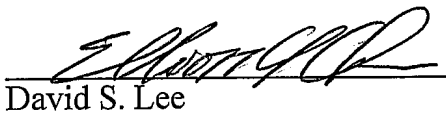
In closing, Applicant's decision not to discuss the differences between the cited art and each dependent claim should not be considered as an admission that Applicant concurs with the conclusions set forth in the Office Action that these dependent claims are not patentable over the disclosure in the cited references. Similarly, Applicant's decision not to discuss differences between the prior art and every claim element, or every comment set forth in the Office Action, should not be considered as an admission that Applicant concurs with the interpretation and assertions presented in the Office Action regarding those claims. Indeed, Applicant believes that all of the dependent claims patentably distinguish over the references cited. Moreover, a specific traverse of the rejection of each dependent claim is not required, since dependent claims are patentable for at least the same

reasons as the independent claims from which the dependent claims ultimately depend.

CONCLUSION

Applicant respectfully requests that the above-proposed amendments be entered and that pending claims 1-8 and 10-40 be allowed. If there are any remaining matters that may be handled by telephone conference, the Examiner is kindly invited to contact the undersigned attorney at the telephone number listed below.

Respectfully Submitted,

Dated: 5-9-08 By: 

David S. Lee
Reg. No. 38,222

Elliott Y. Chen
Reg. No. 58,293

Lee & Hayes, PLLC
421 W. Riverside Ave, Suite 500
Spokane, WA 99201
Phone: (206) 315-4001 x104
or (206) 315-7914
Fax: (206) 315-4004